IJBPAS, April, 2015, 4(4): 1850-1857

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

THE APPLICATION OF DOMINO EFFECT FOR RISK ANALYSIS OF CRITICAL ASSETS IN OIL INDUSTRY

MOHAMMAD NEMATI GOODARZI[1], AHMAD FARMAHINI FARAHANI[2], SEYED EMAD HOSSEINI[3] AND MEHDI TAVAKOLI[4*]

1: Planning manager of institute for International Energy Studies (IIES), Tehran, Iran

2: Director of Research, Institute for International Energy Studies (IIES)

3: Research deputy of institute for International Energy Studies (IIES), Tehran, Iran

4: HSE, NIOC, National Oil Company

***Corresponding Author: E Mail: Tavakolimehdi@yahoo.com**

ABSTRACT

Oil industry is an important section of Country's economic systems. Storage and transportation of large volume of chemical substances as well as large number of staff has subjected it to the security and risk challenges regarding critical assets. This paper aims to accomplish risk analysis for these assets by means of safety risk factor table (SRFT) and step matrix (SMP).SRFT examines the consequences of any threats while SMP investigates on the consequences of domino effect analysis of different threats. This research attempts to carry out the security risk analysis by focusing on the domino effect at a refinery with defined specifications. Finally the risk analysis data are described and some suggestions are provided.

Keyword: Security risk analysis, Critical assets, Domino Effect, Safety Risk Factor table (SRFT), Step Matrix (SMP)

INTRODUCTION

After 9/11 disaster in USA, scholars have paid more attention to the danger of chemical substances. Even though this accident was not directed toward petroleum industries, but these industries are subjected to different critics because of their potentials for serious damages and environmental disasters. Risk analysis for potential threats of oil industry

considers whether the assets of industrial sites need to increase resistance or not. For efficient safety risk analysis, two models have been adopted for risk estimation: SRFT and SMP. The first tries to estimate the risk of any threat separately and the second aims to investigate on domino effect of each threat. The research attempts to introduce the capabilities of this model for risk analysis of critical assets of a refinery as a hypothetical example.

The Hypothetical Example

In this paper the potential threats of a man - made disasters, including terrorism or staffs strike of a refinery (indicated with A) are investigated. The aimed refinery is located near of a chemical fertilizers factory (indicated with Y)

The Profile of Refinery Asset

The refinery (A) is engaged in all of the production procedures. In the other word, the crude oil is entered to the refinery by pipelines and the final products are transported by tankers and rail wagons. The refinery specifications are:

- The location of refinery is poor access.
- The production capacity of refinery is 900000 barrels/day
- The processing sites are not visible from the outside. Only the storage tankers lack a suitable camouflage system
- The refinery has 752 permanent staff but they may increase based on the requirements of any project.

The Refinery Risks

- Consequences of a potential disaster because of large volume of flammable, toxic and corrosive materials
- Recently ,the information system of refinery have been increasingly subjected to the security threats because of increasing the network computers, informational dependence of these computers and availability of information for a large number of staff.
- One of the most vulnerable sections of the refinery (A) for security threats is related to the electronic infrastructures including computers, internet, intra net and information system. In this circumstance, the threats are be able to infiltrate the security system of communication and electronic infrastructures by transferring viruses or Wi-Fi system even from remote place.
- Non isolation of control systems from the other networks is a key mistake. In the other

word, the safety computers are connected to the local network (LAN). Therefore, they can be accessed wirelessly .It intensifies the potential threats. Moreover, there is no identified strategy for staff.

- There is no organizational connection between refinery and chemical fertilizers factory .Consequently, no scheduled program is developed for mutual helps in the emergency cases. The refinery (A) has developed rapport with the local police station; however there is alarming system neither for staff nor for local residents.

Threats and Vulnerabilities

This research enjoys SRFT and SMP for risk analysis of critical assets as mentioned before.

Safety risk factor table (SRFT)

Security risk of a refinery can be analyzed by means of SRFT, by which the all risk factors are ranked from Zero (the lowest risk) to 5 (the highest risk). Ranking is based on the experts' decision. The sum of total scores resulted from **Table (1)**, is used for security risk analysis **(Table 2)**. SRFT examines whether there is necessity of vulnerability and threat analysis or not. According to **Table (2)**, if the total scores be higher than 30, then the vulnerability and threat analysis is imperative. In this inquiry, the total score of the refinery (A) is 37. Therefore, it is necessary to analyze vulnerability accurately in order to mitigate the risks.

Step Matrix (SMP)

SMP is applied to analysis the probably domino effect of a disaster. In the time of a disaster in a refinery, it is probable that the second or more accidents happen.SMP considers the condition of the disasters independent from SRFT.

According to the mechanism of SMP, the matrix counts the number of steps from "i' to "j", therefore the number of steps from "I' to "J" will be [i-j].Each step indicates a single threat which be able to create sever damages.SMP allows to analyze the whole domino effect of a disaster as well as its risks. **Figure (1)** reflects the domino effects from A to H. In refinery (A) the threats scenario is described based on their occurrences from A to H. **A** indicates cyber attacks; **B**, pipeline explosion; **C**, asset explosion; **D** firing, **E** security disclosure. Moreover, the key security fences are:

- Isolation of critical systems from internet and intranet network.
- Access routs control
- Disclosure of information
- Personal Preparation

In the **Figure (1)**, the first matrix only considers the primary disasters. Only two

kinds of primary accidents are being put forwarded: cyber attack and pipeline explosion. However, the number of primary events may increase in the other accidents. The primary disasters can lead to the other accidents which may cause more damages. A cyber attacks (A) leads to asset explosion(C) which leads to firing (D), building damages (G) Pipeline explosion (B) and toxic gas emission (F) subsequently. Non availability of mutual helps (H) may lead to spread the fire to the chemical fertilizers factory

The Domino Tree

A domino tree is drawn to observe the domino effect of disaster. It is resulted from step matrix. By means of domino tree, the probable cases from different scenarios are considered and then, the most probable case is identified. For example, imagine that C and D are resulted independent from B and B is the result of A. **Figure (2)** shows the simplest case of this domino effect. The more number of events, the more complicated trees will be.

The best domino tree is a tree which the total number of its branches is the least. In the other word, the best case for risk analysis is the result of route that possesses the least sum.

Ranking of the Security Barriers

The refinery has established barriers in different sections to cope with the security threats. Barrier ranking refers to allocation of each domino tree to the degree of importance of each security obstacle, including access route control, peripheral control, cyber security and …

Weighting

The weighting procedure is required to prepare a list of security barriers. In this way, a (n×n) matrix is developed .Each (X, Y) is:

- 1- if X=Y
- 3- If X is preferred with low distance
- 5- If X is preferred with relatively high distance
- 7- If X is preferred with high distance
- 9- If X is completely preferred to Y

It is possible to use the mean values (2, 4, 6).It is evident that (Y, X) receives the reversal value. According to the **Table (3)**, it is possible to create a SMP matrix for every scenario. After ranking, the barriers are compared based on their scores.

The vulnerability assessments of the barriers require the following procedures:

- First, normalize the columns. To this end, calculate the sum value for each column, and then divide every matrix elements to the sum value (**Table 4**).

- Normalize the rows. In this way, first calculate the sum value of each row and then divide it to the number of rows (**Table 5**).
- The resultant data of **Table 5** analyze the risk of security obstacle and determines the obstacles which need to increase their resistance. According to this table, the first barrier (Isolation of critical systems from internet and intranet network) and the second one (Access routs control) have gained the highest scores. It means they need to increase resistance more than the other barriers.

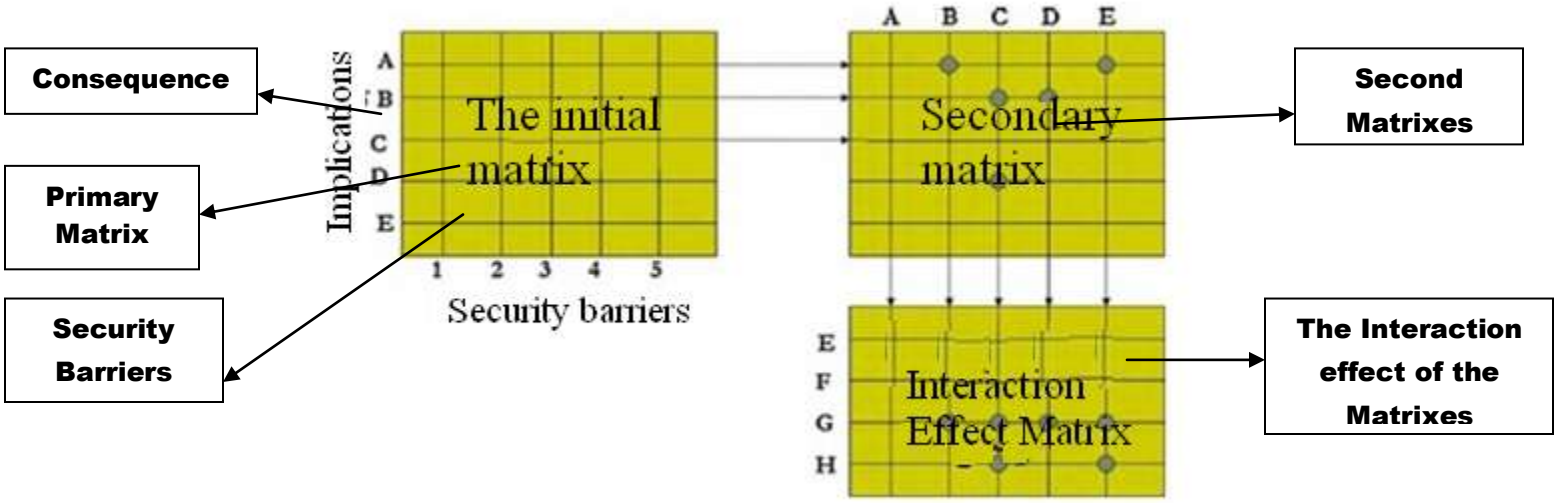

Figure 1: The SMP Matrix

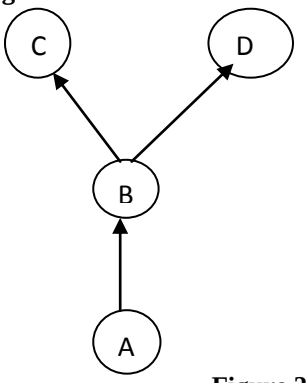

Figure 2: A Simple Domino Tree

Table 1: Safety risk factor (SRFT)

Real Scores	Range of Risk Scores				Risk Factors
1	-	High Density	Urban	Rural	Situation
Visibility	Non visible 0	Low 1,2	Medium 3,4	High 5	1
Assets	Low 1	Medium 2	High 3,4	Very high 5	1
Possession	Privative	Common		Governmental	5

	1	**2,3**		**4,5**	
Terrorism Background of the Region	**Non 0**	**Rarely 1,2,3**		**Very 4,5**	**5**
Existing Security Actions	**High**	**Normal**		**Weak**	**3**
Availability Control	**1**	**2,3**		**4,5**	**2**
Peripheral Supporting	**1**	**2,3**		**4,5**	**2**
Risk Mitigation	**1**	**2,3**		**4,5**	**2**
Appropriate Lighting	**1**	**2,3**		**4,5**	**3**
Training and Personal Preparations	**Good 1**	**Medium 2,3**		**Weak 4,5**	**2**

Table 2: Safety Risk Factors

Real Risk Score	Status qua of Security Risk
<15	**Low**
16-30	**Medium**
31-45	**High**
45>	**Very High**

Table 3: The SMP Matrix for Security Barriers

	1	**2**	**3**	**4**	**5**
1	**1**	**1/3**	**2**	**4**	**8**
2	**3**	**1**	**5**	**6**	**7**
3	**1/3**	**1/5**	**1**	**7**	**5**
4	**¼**	**1/6**	**1/7**	**1**	**5**
5	**1/8**	**1/7**	**1/5**	**1/5**	**1**

Table 4: Columns Normalizing

	1	**2**	**3**	**4**	**5**
1	**0.2**	**0.18**	**0.23**	**0.22**	**0.30**
2	**0.61**	**0.54**	**0.59**	**0.32**	**0.6**
3	**0.10**	**0.10**	**0.11**	**0.38**	**0.19**
4	**0.05**	**0.09**	**0.01**	**0.05**	**0.19**
5	**0.02**	**0.07**	**0.02**	**0.01**	**0.03**

Table 5: Rows Normalizing

	Sum value	Sum value/5
1	**1.13**	**0.23**
2	**2.23**	**0.46**
3	**0.88**	**0.18**
4	**0.39**	**0.07**
5	**0.15**	**0.07**

CONCLUSIONS

In the oil industry, the disasters caused by the security threats possess the domino effects. Each disaster may potentially lead to the other accidents which may increase the vulnerability of the critical assets. Implementing a risk analyzing system for effective risk management of critical infrastructure requires determining the disaster consequences. Therefore, it is

necessary to analyze the probable consequences for each risk. This research attempts to analyze the consequences by means of a domino tree. A domino tree is developed through SMP matrix. To this end, it is necessary to list the risk factors in a safety risk factor table (SRFT).This table includes disasters, infiltration routs and the interaction effect of disasters. If threats and vulnerabilities could be determined easily there is no need for broad analyzing, because of time saving and cost decreasing. The proposed model of this research can investigate on domino effect of all probable threats and risks. The mathematical calculations of this methodology have the capability to be applied for a large number of industries, including electronic and atomic industries. The design of SMP, domino tree and the defined ranking procedures are not merely nature dependant. The individuals' skill, knowledge and experiences are very important for risk analysis of critical assets. Consequently, the abovementioned methodology is flexible and can be applied in different circumstances. The application of this methodology is recommended for risk analysis of assets in complicated industries, in which the suitable risk management could be facilitating.

REFERENCES

[1] S. Bajpai, J.P. Gupta, 2005,Protecting chemical plants from terrorist attacks,Chem.Weekly L34, 209 213.

[2] S. Bajpai, J.P. Gupta, 2005, Securing oil and gas infrastructure, J. Pet. Sci. Eng. 55174 186.

[3] American Petroleum Institute (API), 2003, Security Guidelines for the Petroleum Industry, Washington, DC.

[4] Abbasi, S.A. and Khan, F.I., 2001, An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. Journal of Loss Prevention in the Process Industries.

[5] Bajpai, S. and Gupta, J.P., 2005, Site security for chemical process industry, Journal of Loss Prevention in the Process Industries.

[6] Aven T, Vinnem JE, Wiencke HS., 2006, A decision framework for HESmanagement,ReliabEngSystSaf.

[7] Kristensen V, Aven T, Ford D., 2006, A new perspective on Renn&Klinke sapproach to risk evaluation and risk management, ReliabEngSystSaf.

[8] Garrick BJ, *et al*., 2004, Confronting the risks of terrorism: making the right decisions.

[9] Reliab Eng SystSaf.